UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/378,226	08/19/1999	MARK D. RIGGINS	40827.00011	8867

7590 02/21/2006

Jinntung Su
MANATT, PHELPS & PHILLIPS LLP
1001 Page Mill Road
Building 2
Palo Alto, CA 94303

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 02/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/378,226	RIGGINS, MARK D.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 December 2003* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 14 November 2005.

2. Claims 1-30 are pending in the application.

3. Claims 1-30 have been rejected.

Response to Amendment

4. The examiner approves of the amendment made to claim 30. There are no more misspellings in the claim. The examiner withdraws the objection to claim 30.

Response to Arguments

5. Applicant's arguments filed 14 November 2005 have been fully considered but they are not persuasive.

The applicant traverses that there is an omitted step for "deriving a key". The applicant argues that "hashing at least one of the hint and the password" derives the key.

The examiner respectfully disagrees. The applicant merely has a limitation stating "deriving the key by hashing at least one of the hint and the password". However, the examiner asserts that it is not known to a person having ordinary skill in the art how a key is created by hashing a hint and a password. There are also no steps included for deriving a key from a decryption downloadable.

On page 8, regarding claims 1 and 8, the applicant argues that Grawrock does not disclose, "performing a hashing algorithm on the hint and the password to generate a key".

The examiner respectfully disagrees. Grawrock discloses hashing the question and the bona fide answer (i.e. password) to form the encryption key.

On page 8, regarding claim 4, the applicant argues that Grawrock does not disclose, "a key generator coupled to the user interface for performing a hashing algorithm on a hit and the password to generate a key".

The examiner respectfully disagrees. As discussed above, Grawrock discloses hashing the question and the bona fide answer (i.e. password) to form the encryption key.

On page 8, regarding claim 11, the applicant argues that Grawrock does not disclose, "receiving a request to store encrypted data from a client".

The examiner respectfully disagrees. A user must authenticate themselves with a password to access the computer system. By logging on the system to store encrypted data, the act of logging onto the computer is the request to store encrypted data.

On page 8, regarding claim 12, the applicant argues that Grawrock does not disclose, "memory coupled to the web server for storing a hint corresponding to the encrypted data and needed to regenerate the key from the client and the encrypted data".

The examiner respectfully disagrees. Grawrock teaches a server for providing hints to recover forgotten passwords. A hash of the hint and password will generate the key to encrypt data.

On pages 8-9, regarding claims 13, 15 and 16, the applicant argues that Grawrock does not disclose, "performing a hashing algorithm on the password and the hint at the client to generate a key".

The examiner respectfully disagrees. As discussed above, Grawrock discloses hashing the question and the bona fide answer (i.e. password) to form the encryption key.

On page 9, regarding claim 19, the applicant argues that Grawrock does not disclose, "receiving identification of encrypted data".

The examiner respectfully disagrees. Grawrock discloses that the encrypted data is identified by the index value.

On page 9, regarding claim 3, the applicant argues that Challener does not disclose, "performing a hashing algorithm on the hint and the password to generate a key, wherein the step of performing a hashing algorithm includes hashing the password to derive a first secret, hashing the first secret to derive a second secret, hashing the hint and the first secret to generate an intermediate index, and hashing the intermediate index and the second secret to generate the key".

The examiner respectfully disagrees. Challener discloses that a secret key is formed from the hash of the hint and the password. The secret key is derived from a first hash of the password. The result is hashed with the hint to form the second secret. The password constitutes the intermediate index. Hashing the intermediate index forms all further encrypting keys.

On pages 9-10, regarding claim 7, the applicant argues that Challener does not disclose, "a key generator coupled to the user interface for performing a hashing algorithm on a hint and the password to generate a key wherein the key generator hashed the password to derive a first secret".

The examiner respectfully disagrees. As discussed above, hashing the password with the hint generates the first secret key.

On page 10, regarding claims 20, 21 and 26, the applicant argues that Challener does not disclose, "deriving an intermediate index from the first secret and the hint".

The examiner respectfully disagrees. As discussed above, Challener discloses that a secret key is formed from the hash of the hint and the password. The secret key is derived from a first hash of the password. The result is hashed with the hint to form the second secret. The password constitutes the intermediate index. Hashing the intermediate index forms all further encrypting keys.

On page 10, regarding claim 24, the applicant argues that Challener does not disclose, "an index generator coupled to the user interface for generating an intermediate index from a hint received from a server and a secret derived from the password".

The examiner respectfully disagrees. As discussed above, Challener discloses that a secret key is formed from the hash of the hint and the password. The secret key is derived from a first hash of the password. The result is hashed with the hint to form the second secret. The password constitutes the intermediate index. Hashing the intermediate index forms all further encrypting keys.

On page 10, regarding claims 29 and 30, the applicant argues that Challener does not disclose, "a decryption downloadable for generating an intermediate index from a password and a hint".

The examiner respectfully disagrees. Challener discloses that the configuration changes are the decrypted downloadables. They are used for generating an intermediate index from a password and a hint.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 19 and 20 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01.

The omitted steps are: steps for "deriving a key". The applicant recites "sending a decryption downloadable for deriving a key from a password and a hint". However, there are no steps recited in how the key is actually derived. Additionally, there is no end result to both claims.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 2, 4-6 and 8-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Grawrock U.S. Patent No. 6,360,322 B1.

As to claims 1 and 8, Grawrock discloses a method, comprising:

obtaining a hint [column 5, lines 1-42];

obtaining a password [column 5, lines 1-42];

sending the hint to a client [column 5, lines 1-42];

performing a hashing algorithm on the hint and the password to generate a key [column 6 line 52 to column 7 line 27];

encrypting data using the key [column 6 line 52 to column 7 line 27];

sending the encrypted data to a server for storage [column 6 line 52 to column 7 line 27]; and

As to claim 2, Grawrock discloses that the step of performing a hashing algorithm includes hashing the password [column 6 line 52 to column 7 line 27].

As to claim 4, Grawrock discloses a system, comprising:

a user interface for obtaining a password [column 5, lines 1-42];

a key generator coupled to the user interface for performing a hashing algorithm on a hint and the password to generate a key [column 6 line 52 to column 7 line 27];

an encryption engine coupled to the key generator for encrypting data using the key [column 6 line 52 to column 7 line 27];

a communications module coupled to the engine for sending the encrypted data and the hint to a server for storage [column 6 line 52 to column 7 line 27].

As to claim 5, Grawrock discloses a hint generator for generating the hint [column 5, lines 1-42].

As to claim 6, Grawrock discloses that the key generator hashes the password [column 6 line 52 to column 7 line 27].

As to claim 9, Grawrock discloses that the system includes code stored on a computer-readable storage medium [column 2, lines 47-53].

As to claim 10, Grawrock discloses that the system includes code embodied in a carrier wave [column 2, lines 47-53].

As to claim 11, Grawrock suggests receiving a request to store encrypted data from a client [column 2, lines 54-62]. Grawrock discloses sending an encryption downloadable for deriving a key to encrypt data to the client [column 3, lines 5-13]. Grawrock teaches receiving encrypted data that was encrypted by the encryption downloadable from the client [column 3, lines 14-22]. Grawrock discloses obtaining a hint corresponding to the encrypted data and needed for regenerating the key and storing the hint and the encrypted data [column 6 line 52 to column 7 line 27].

As to claim 12, Grawrock discloses an encryption downloadable for deriving an encryption key from a password and a hint [column 5, lines 1-42]. Grawrock suggests a web server for interfacing with a client for sending the encryption downloadable to the client [column 3, lines 5-13]. Grawrock discloses receiving encrypted data that was encrypted by the encryption downloadable from the client [column 3, lines 5-13]. Grawrock suggests memory coupled to the web server for storing a hint corresponding to the encrypted data and needed to regenerate the key from the client and the encrypted data [column 5, lines 1-42].

As to claims 13 and 16, Grawrock discloses a method, comprising:

obtaining a password [column 5, lines 1-42];

sending encrypted data and a hint corresponding to the encrypted data from a server to a client [column 5, lines 1-42]; and

performing a hashing algorithm on the password and the hint at the client to generate a key for decrypting the encrypted data [column 6 line 52 to column 7 line 27].

As to claim 14, Grawrock discloses that the step of performing a hashing algorithm includes hashing the password [column 6 line 52 to column 7 line 27].

As to claim 15, Grawrock discloses a system, comprising:

a user interface for obtaining a password [column 5, lines 1-42];

a communications module for sending encrypted data and a hint corresponding to the encrypted data from a server to a client [column 5, lines 1-42]; and

a key generator for performing a hashing algorithm on the password and the hint at the client to generate a key for decrypting the encrypted data [column 6 line 52 to column 7 line 27].

As to claim 17, Grawrock discloses that the system includes code stored on a computer-readable storage medium [column 2, lines 47-53].

As to claim 18, Grawrock suggests that the system includes code embodied in a carrier wave [column 2, lines 47-53].

As to claim 19, Grawrock discloses a method, comprising:

receiving identification of encrypted data [column 2, lines 54-62];

sending a decryption downloadable for deriving a key from a password and a hint to a client [column 5, lines 1-42];

sending a hint corresponding to the encrypted data to the client [column 5, lines 1-42]; and

deriving the key by hashing at least one of the hint and the password [column 6 line 52 to column 7 line 27].

8. Claims 3, 7 and 20-30 are rejected under 35 U.S.C. 102(e) as being anticipated by Challener et al U.S. Patent No. 6,470,454 B1.

As to claim 3, Challener et al discloses a method, comprising:

obtaining a hint [column 5, lines 28-50];

obtaining a password [column 5, lines 28-50];

performing a hashing algorithm on the hint and the password to generate a key, wherein the step of performing a hashing algorithm includes hashing the password to derive a first secret [column 5, lines 51-58], hashing the first secret to derive a second secret, hashing the hint and the first secret to generate an intermediate index, and hashing the intermediate index and the second secret to generate the key [column 5 line 59 to column 6 line 33];

encrypting data using the key [column 5 line 59 to column 6 line 33]; and

sending the encrypted data to a server for storage [column 5 line 59 to column 6 line 33].

As to claim 7, Challener et al discloses a system, comprising:

a user interface for obtaining a password; [column 5, lines 28-50]

a key generator coupled to the user interface for performing a hashing algorithm on a hint and the password to generate a key wherein the key generator

hashes the password to derive a first secret [column 5, lines 51-58], hashes the first secret to derive a second secret, hashes the hint and the first secret to generate an intermediate index, and hashes the intermediate index and the second secret to generate the key [column 5 line 59 to column 6 line 33];

an encryption engine coupled to the key generator for encrypting data using the key [column 5 line 59 to column 6 line 33]; and

a communications module coupled to the engine for sending the encrypted data to a server for storage [column 5 line 59 to column 6 line 33].

As to claim 20, Challener et al discloses a method, comprising:

obtaining a password [column 5, lines 28-50];

deriving a first secret from the password [column 5, lines 28-50];

receiving a hint corresponding to data to be decrypted from a server [column 5, lines 28-50];

deriving an intermediate index from the first secret and the hint [column 5 line 59 to column 6 line 33]; and

sending the intermediate index to the server [column 5 line 59 to column 6 line 33].

As to claim 21, Challener et al discloses a client-based method, comprising:

obtaining a password [column 5, lines 28-50];

deriving a first secret from the password [column 5, lines 28-50];

receiving a hint corresponding to data to be decrypted from a server [column 5, lines 28-50];

deriving an intermediate index from the first secret and the hint [column 5 line 59 to column 6 line 33]; and

sending the intermediate index to the server [column 5 line 59 to column 6 line 33].

As to claim 22, Challener et al discloses that deriving the first secret includes hashing the password [column 5, lines 28-50].

As to claim 23, Challener et al discloses that deriving an intermediate index includes hashing the first secret and the hint [column 5 line 59 to column 6 line 33].

As to claim 24, Challener et al discloses a system, comprising:

a user interface for obtaining a password [column 5, lines 28-50];

an index generator coupled to the user interface for generating an intermediate index from a hint received from a server and a secret derived from the password [column 5 line 59 to column 6 line 33]; and

a communications engine coupled to the index generator for sending the intermediate index to the server [column 5 line 59 to column 6 line 33].

As to claim 25, Challener et al discloses that the index generator generate the intermediate index by hashing the hint and the secret [column 5 line 59 to column 6 line 33].

As to claim 26, Challener et al discloses a system, comprising:

means for obtaining a password [column 5, lines 28-50];

means for deriving a first secret from the password [column 5, lines 28-50];

means for receiving a hint corresponding to data to be decrypted from a server [column 5, lines 28-50];

means for deriving an intermediate index from the first secret and the hint [column 5 line 59 to column 6 line 33]; and

means for sending the intermediate index to the server [column 5 line 59 to column 6 line 33].

As to claim 27, Challener et al discloses that the system includes code stored on a computer-readable storage medium [column 3, lines 22-35].

As to claim 28, Challener et al suggests that the system includes code embodied in a carrier wave [column 3, lines 22-35].

As to claim 29, Challener et al discloses a server-based method, comprising:

receiving an indication of encrypted data to be decrypted [column 6, lines 21-57];

transmitting to a client a hint corresponding to the indication [column 6, lines 21-57], and a decryption downloadable for deriving an intermediate index from a password and the hint [column 6, lines 21-57];

receiving the intermediate index from the client [column 5 line 59 to column 6 line 33];

deriving a decryption key from a second secret corresponding to the user and the intermediate index [column 5 line 59 to column 6 line 33].

As to claim 30, Challener et al discloses a system, comprising:

a second secret corresponding to a user [column 6, lines 21-57];

a decryption downloadable for generating an intermediate index from a password and a hint [column 6, lines 21-57];

a web server for receiving an indication of encrypted data to be decrypted [column 5 line 59 to column 6 line 33], for transmitting the decryption downloadable and a hint corresponding to the indication to a client [column 5 line 59 to column 6 line 33], and for receiving an intermediate index from the client [figure 6]; and

a server-resident module for deriving a key for decrypting the encrypted data from the second secret and the intermediate index [column 5 line 59 to column 6 line 33].

Conclusion

9. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy AM
February 13, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100